FREEDMAN & Associates
REGISTERED PATENT AND TRADEMARK AGENTS

Gordon Freedman, LLB, Patent* and Trademark Agent
Computer and Systems Engineer

Neil Teitelbaum, Patent Agent*
Electrical Engineer

Karen Stauss, Patent Agent

Juergen Fuchs, Ph.D. Mech.Eng

Jennifer McCann, Ph.D. Chem

* Registered in Canada And U S

54 Cimarron Cr
Nepean, Ontario
Canada K2G 6C9
Tel(613) 730 - 5151
Fax(613) 730 - 4141

Email gordon@patents org
http //www canpatent com

jc662 U.S. PTO
03/09/00

jc678 U.S. PTO
09/522043
03/09/00

March 8, 2000

The Commissioner of Patents and Trademarks
Washington, D.C. 20231
U.S.A.

Sir:

Re: New United States CONTINUATION-IN-PART Patent Application
Title: RANDOM NUMBER GENERATOR AND METHOD FOR SAME
Inventor(s)): Borza et al
Our File: 12-19 US CIP(2)

This is a Request for filing of a new CIP patent application of U.S. CIP Serial No: 09/023,460 filed February 13, 1998 and U.S. Serial No: 08/728,549 filed October 9, 1996 in the United States.

Enclosed for the filing of a new patent application in the United States are:

1) Assignment and Assignment cover page;
2) Declaration signed by the Inventor(s);
3) Abstract of the Disclosure, **26** pages of specification (excluding drawings), including **20** claims, **5** being independent;
4) Formal drawings including **10** figures;
5) Small entity form;
6) A cheque in the sum of **$423.00** to cover the filing fee;
7) A cheque in the amount of **$40.00** to cover assignment fee.

Convention priority is claimed under 35 USC 119 with respect to U.S. Patent Appln. No: 08/728,549 filed October 9, 1996 and U.S. CIP Serial No: 09/023,460 filed February 13, 1998

I will be pleased to receive the filing particulars of this application. Enclosed is a self-addressed postcard to indicate that the application has been received by the USPTO.

Please charge any additional fees or credit overpayment to Deposit Account No: 501142.

Respectfully submitted,

G Fre

Gordon Freedman
Registered Patent Agent
Regn No: 41, 553

/mdb

VERIFIED STATEMENT CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) & 1.27(c))-SMALL BUSINESS CONCERN	Attorney Docket No. 12-19 US CIP(2)

Applicant or Patentee: Stephen J. BORZA; Gordon FREEDMAN

Serial or Patent No:

Filed or Issued:

Title: **RANDOM NUMBER GENERATOR AND METHOD FOR SAME**

I hereby declare that I am
[ ] the owner of the small business concern identified below:
[X] an official of the small business concern empowered to act on behalf of the concern identified below:

NAME OF SMALL BUSINESS CONCERN **Dew Engineering and Development Limited**

ADDRESS OF SMALL BUSINESS CONCERN **3429 Hawthorne Road, Ottawa, Ontario, Canada K1G 4G2**

I hereby declare that the above identified small business concern qualifies as a small business concern as defined in 13 CFR 121.12, and reproduced in 37 CFR 1.9(d), for purposes of paying reduced fees to the United States Patent and Trademark Office, in that the number of employees of the concern, including those of its affiliates, does not exceed 500 persons. For purposes of this statement, (1) the number of employees of the business concern is the average over the previous fiscal year of the concern of the persons employed on a full-time, part-time or temporary basis during each of the pay periods of the fiscal year, and (2) concerns are affiliates of each other when either, directly or indirectly, one concern controls or has the power to control the other, or a third party or parties controls or has the power to control both.

I hereby declare that rights under contract or law have been conveyed to and remain with the small business concern identified above with regard to the invention, described in:

[X] the specification filed herewith with title as listed above.
[ ] the application identified above.
[ ] the patent identified above.

If the rights held by the above identified small business concern are not exclusive, each individual, concern or organization having rights in the invention must file separate verified statements averring to their status as small entities and no rights to the invention are held by any person, other than the inventor, who would not qualify as an independent inventor under 37 CFR 1.9(c) if that person made the invention, or by any concern which would not qualify as a small business concern under 37 CFR 1.9(d), or a nonprofit organization under 37 CFR 1.9(e).

Each person, concern or organization having any rights in the invention is listed below:

[X] No such person, concern, or organization exists.
[ ] Each such person, concern, or organization is listed below.

Separate verified statements are required from each named person, concern organization having rights to the invention averring to their status as small entities. (37 CFR 1.27)

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 CFR 1.28 (b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that wilful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such wilful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

NAME OF PERSON SIGNING Kent R Foster

TITLE OF PERSON IF OTHER THAN OWNER Chief Operating Officer

ADDRESS OF PERSON SIGNING 3429 Hawthorne Road, Ottawa, Ontario, Canada K1G 4G2

SIGNATURE _____ DATE 20.12.99

Random Number Generator and Method for Same

This is a continuation-in-part from U.S. Patent application 09/023,460 filed February 13, 1998 which further claims priority from U.S. Patent Application 08/728,549 filed October 9, 1996.

Field of the Invention

This invention relates generally to random number generation and more particularly relates to a method of generating a number within a random sequence of numbers using noise presented to or from within a charge coupled device (CCD) or the like.

Background of the Invention

Computer security is fast becoming an important issue. With the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file access is growing. One method of providing security from unauthorized access to files is by implementing encryption and cipher techniques. These techniques convert data into other corresponding data forms in a fashion that is reversible. Once encrypted, the data is unintelligible unless first decrypted. RSA, DES, PGP, and CAST are known encryption techniques that are currently believed to provide sufficient security for computer communications and files.

Each of these encryption techniques uses a key or cipher. Such a key is crucial to the encryption/decryption process. Anyone with a correct key, can access information that has previously been encrypted using that key. The entry of the key from the keyboard is impractical since a key remembered by a user for entry is liable to be discovered by an individual desiring unauthorized access to existing encrypted files.

In DES encryption, the key is a numerical value, for example 56 bits in length. Such a key can be used to encrypt and subsequently to decrypt data. The security of the

data once encrypted is sufficient that the key is required to access the data in an intelligible form. Thus, the security of the data is related to the security of the key.

In an optical fingerprint input transducer or sensor, the finger under investigation is usually pressed against a flat surface, such as a side of a glass plate, and the ridge and valley pattern of the finger tip is sensed by a sensing means such as an interrogating light beam.

Various optical devices are known which employ prisms upon which a finger whose print is to be identified is placed. The prism has a first surface upon which a finger is placed, a second surface disposed at an acute angle to the first surface through which the fingerprint is viewed and a third illumination surface through which light is directed into the prism. In some cases, the illumination surface is at an acute angle to the first surface, as seen for example, in US Patents 5, 187, 482 and 5, 187, 748. In other cases, the illumination surface is parallel to the first surface, as seen for example, in US Patents 5, 109, 427 and 5, 233, 404. Fingerprint identification devices of this nature are generally used to control the building-access or information-access of individuals to buildings, rooms, and devices such as computer terminals.

In capacitive fingerprint imaging devices, a fingertip is pressed against an array of sensing electrodes. Each electrode forms one of two electrodes in a capacitor. Each capacitor is generally pre-charged to provide a known voltage. The placement of the fingertip on the sensing electrodes results in changes to the induced voltages or capacitances and therefore allows for imaging of the fingerprint. Devices of this type are well known in the art.

The use of random numbers has become popular in many aspects of computer science. An annealing algorithm generates an entire process based on an initial random seed. The seed allows the process to be repeated, but its random nature allows the annealing process to run differently each time. In encryption technology, random keys are also used for generating private and public keys. Unfortunately, computers are only

capable of generating pseudo random numbers. These numbers may follow known sequences or they may rely on date and time information making them predictable.

Several electronic approaches to random number generation have been proposed. It is known to use a resistive circuit that generates a voltage or current to be measured that lies at an exact value. Voltages above and below the value are interpreted as a one and a zero, respectively. Of course, it will be apparent to those of skill in the art that the selection of one to be above the threshold is arbitrary and that the respective interpretation can be otherwise. The random nature of the binary value is ensured based on the laws of quantum physics. Unfortunately, such a system is influenced by external factors such as temperature, humidity, etc. Also, electronic random number generators for use with a computer are often costly.

When conditions change, existing devices often become unreliable. For example, a resistance based device often produces a sequence of "random" numbers of a dubious nature when temperature changes are significant. As is well known, this is often the case within computer systems, where bright lights are used, near doorways, in electronic devices, in automobiles, and so forth. As such, a more flexible random number generating device and method is needed.

It is, therefore, an object of this invention to provide a cost effective means of generating a number within a random sequence of numbers having a configurable distribution.

It is further an object of the invention to provide means of generating a number within a random sequence of numbers using already existing devices connected to a computer and used for other purposes such as biometric input devices or touchpads.

Summary of the Invention

In accordance with the invention, there is provided, a method of generating a number within a random sequence of numbers using an imaging device comprising a transparent

layer for transmitting impinging light of an image provided to the imaging device and an array of imaging sensors within an integrated circuit affixed to a layer of substrate for sensing the transmitted light, the method comprising the steps of:

sensing with the array of imaging sensors an image provided to the device;

providing image data corresponding to the sensed image, wherein the image data comprise an array of pixels, each pixel provided by one imaging sensor of the imaging sensor array; and,

if no image is provided to the device:

sensing, with a first imaging sensor, a first signal to provide first sensed data, wherein at least a portion comprises noise presented to or from within the device;

sensing, with a second imaging sensor, a second signal to provide second sensed data, wherein at least a portion comprises noise presented to or from within the device;

determining a noise based value from the noise portion within each of the first sensed data and the second sensed data; and,

based on the noise based value providing the number within the random sequence of numbers.

A further embodiment comprises the additional steps of:

sensing, with a third imaging sensor, a third signal to provide third sensed data, wherein at least a portion comprises noise presented to or from within the device;

sensing, with a fourth imaging sensor, a fourth signal to provide fourth sensed data, wherein at least a portion comprises noise presented to or from within the device;

determining a first noise based value from the noise portion within each of the first sensed data and the second sensed data;

determining a second noise based value from the noise portion within each of the third sensed data and the fourth sensed data;

based on the second noise based value modifying the first noise based value; and,

based on the modified noise based value providing the number within the random sequence of numbers.

In accordance with another aspect of the invention there is further provided a method of generating a number within a random sequence of numbers using an imaging device comprising a transparent layer for transmitting impinging light of an image provided to the imaging device and an array of imaging sensors within an integrated circuit affixed to a layer of substrate for sensing the transmitted light, the method comprising the steps of:

sensing with the array of imaging sensors an image provided to the device;

providing image data corresponding to the sensed image, wherein the image data comprise an array of pixels, each pixel provided by one imaging sensor of the imaging sensor array; and,

if no relevant image information is provided to at least two imaging sensors of the array of imaging sensors:

sensing, with a first imaging sensor of the at least two imaging sensors, a first signal to provide first sensed data wherein at least a portion comprises noise presented to or from within the device;

sensing, with a second imaging sensor of the at least two imaging sensors, a second signal to provide second sensed data wherein at least a portion comprises noise presented to or from within the device;

determining a noise based value from the noise portion within each of the first sensed data and the second sensed data; and,

based on the noise based value providing the number within the random sequence of numbers.

In accordance with yet another aspect of the invention there is provided a method of generating a number within a random sequence of numbers using a device comprising an array of sensing electrodes, each sensing electrode being one of a pair of electrodes forming a capacitor, the method comprising the steps of:

sensing with the array of sensing electrodes an image of an object in contact with or in close proximity of the device, wherein the sensing electrodes sense a change of capacitance induced by the object;

providing image data corresponding to the sensed image by measuring the change of capacitance; and,

if no image is provided to the device:

sensing, with a first sensing electrodes, a first signal to provide first sensed data, wherein at least a portion comprises noise presented to or from within the device;

sensing, with a second sensing electrodes, a second signal to provide second sensed data, wherein at least a portion comprises noise presented to or from within the device;

determining a noise based value from the noise portion within each of the first sensed data and the second sensed data; and,

based on the noise based value providing the number within the random sequence of numbers.

In accordance with the invention there is provided an imaging device used for generating a number within a random sequence of numbers comprising:

a transparent layer for transmitting impinging light in dependence upon an image provided to the imaging device;

an array of imaging sensors within an integrated circuit affixed to a layer of substrate for sensing the transmitted light and for providing an array of pixels corresponding to the sensed image, each pixel provided by one imaging sensor of the imaging sensor array and comprising a signal in dependence upon input information provided to the imaging sensor, wherein at least a portion of the signal comprises white noise presented to or from within the imaging sensor; and,

a processor for receiving the signals from at least two imaging sensors of the imaging sensor array and for determining a value based on the portions of the signals comprising white noise.

In accordance with another aspect of the invention there is provided a device used for generating a number within a random sequence of numbers comprising:
an array of sensing electrodes, each sensing electrode being one of a pair of electrodes forming a capacitor, for sensing an image of an object in contact with or in close proximity of the device by sensing a change of capacitance induced by the object and for providing image data corresponding to the sensed image; and,
a processor for receiving the signals from at least two sensing electrodes of the array of sensing electrodes and for determining a value based on the portions of the signals comprising white noise.

The advantages of a system in accordance with this invention are numerous. For example, random number generation will vary effectively from computer to computer thereby decreasing chances of predicting random number values.

It is a significant advantage that a device according to the invention is capable of calibration and reconfiguration during normal use.

It is a significant advantage of the present invention that a single sensor array serves multiple purposes.

Brief Description of the Drawings

An exemplary embodiment of the invention will now be discussed in conjunction with the attached drawings in which:

Fig. 1 is a block diagram of a known biometric sensing device with an additional diffusing cover thereon according to the present invention;

Fig. 1a is a schematic diagram of a charged coupled device;

Fig. 2 is simplified diagram of a capacitive fingerprint imaging device;

Fig. 3 is a simplified diagram of an optical fingerprint imaging device with an additional diffusing cover thereon according to the present invention;

Fig. 4a is a flow diagram of a method according to the present invention;

Fig. 4b is a flow diagram of another method according to the present invention;

Fig. 4c is a flow diagram of another method according to the present invention;

Fig. 4d is a flow diagram of yet another method according to the present invention;

Fig. 4e is a flow diagram of yet another method according to the present invention; and

Fig. 5 is a flow diagram of a method of calibrating a device according to the present invention.

Detailed Description

Throughout the specification and claims, the term a number within a random sequence of numbers is defined to mean a number that is not predictable. For example, the definition of random number generation in the Computer Dictionary, 1993, Microsoft Press is "The creation of a number or sequence of numbers characterized by unpredictability so that no number is any more likely to occur at a given time or place in the sequence than any other." Of course this refers to a random number generator producing a flat distribution of random values. Other distributions are known and do not reduce the random nature of the sequence. For example, a die with two faces having a 1 thereon has twice the likelihood of resulting in a 1 and yet results in a random sequence when thrown repeatedly. A random number as defined above, is a number in a sequence of numbers wherein the sequence exhibits certain statistical behaviors. For example, a random sequence generated by a random number generator is non-repeating, non-predictable, and non-reproducible.

The term non-deterministic random number is defined to mean a number that is not determinative based solely on an input to a system and forms a subset of random numbers.

A pseudo-random number is a deterministic number determined in a fashion that causes it to appear random when in fact it is not; it is repeatably determined and given a seed value, can be regenerated using a same pseudo-random number generator

A near random number is a number that is a random number but that does not subscribe to a desired distribution either because the distribution varies over time or because it is statistically predictable in some way.

A device, shown in Fig. 1, comprises a biometric sensing device 1 through which biometric input in the form of a fingerprint is received. Similar devices absent the diffusing cover 20 are known in the art of biometric sensing. In use a fingertip is placed on the biometric sensing device 1 and illuminated. Light from a light source 6 is reflected by the fingertip and is then reflected off several mirrors 12 prior to passing through a lens 13 to focus upon an imaging device 2, such as a charge coupled device (CCD). The number of mirrors used is optional but is chosen so as to limit other light sources (noise) and to limit image degradation. Alternatively, no mirrors are present and the light reflected by the fingertip is passed directly through the lens 13. The lens 13 is spaced from the CCD 2 so that an image is focused upon the CCD 2. Such optical focus is well known in the art.

Referring to Fig. 1a a schematic diagram of a CCD 2 is shown. The CCD 2 comprises an array of imaging sensors 62 (for example an array of 200x300) made of light sensitive semiconductor material within an integrated circuit affixed to a layer of substrate 64 such as silicon. The integrated circuit further comprises connections 66 to each imaging sensor. A light sensitive material often used in CCDs is, for example, doped polysilicon. Photons impinging onto the sensor 62 free electrons from the sensor's crystal lattice. Therefore, an electrical signal proportional to the amount of photons, that

is, proportional to light intensity, is provided by the sensor 62 and transmitted via the connection 66 to address and output generating means 68. The CCD 2 further comprises a transparent layer 60 for transmitting the light of an image onto the array of imaging sensors 62 and for protecting the integrated circuitry.

Alternatively, a complementary metal oxide semiconductor (CMOS) imaging device may be used. The recently developed CMOS imaging device comprises a similar structure as the CCD shown in Fig. 1a, but it is expected that use of different materials provide a significant reduction of production costs.

The CCD 2 is capable of converting an incident optical image into electrical signals; such use of CCDs is known. Output from the CCD is an analog electrical signal. The output electrical signal is passed to circuit 50 which adjusts the signal as necessary to meet a pre-selected analog video signal standard which is then transmitted by the circuit 50 via the carrier means 7 to a connection means 9 which in turn is connected to a frame grabber 22. The frame grabber 22 is commonly a peripheral card installed within a computer 10.

When no fingertip is located on the prism 1, the CCD 2 captures ambient light. Some of this light is from sources external to the biometric scanner. Other light is from a light source within the biometric scanner. Yet another source of captured light is backlight. The exact percentage from each is unknown and somewhat random within a range of values. Calibration of the device in a particular environment or providing the device with a cover 20 provides some indication of a percentage of a signal derived from ambient light or light sources and a percentage of light derived from other sources such as noise.

The CCD 2 has a large number of imaging sensors within the device (for example an array of 200x300) in order to provide sufficient resolution of an image (for example an array of 200x300 pixels). To generate a single binary value, all 60, 000 pixels can be summed and averaged. This value will fall between 0 and the depth of the pixels (in value

and not in bits). Once calibrated, a value will map onto a bit of "1" or a bit of "0" and therefore result in the selection of a binary random number.

Essentially, the invention relies on the existence of white noise - random noise - at the imaging sensors and filters out a known signal of ambient diffused light or of a known pattern in the case of a device provided with a cover. The use of a CCD as the imaging device is rendered cost effective both because CCD costs are falling and because a CCD is known to be used with a computer for other applications such as biometric sensing. Multiple uses of a CCD allow each function to bear only a portion of the cost of the electronic device. Further, the use of a CCD provides numerous imaging sensors and thereby allows for software configuration, calibration, and selection of a desired distribution of values for the random sequence.

Referring to Fig. 2, a capacitive fingerprint imager is shown. Similar devices are used in biometric sensing and in touchpads. The imaging device comprises an array of sensing electrodes 78 spaced apart to prevent interference. Each sensing electrode 78 forms one of two electrodes in a capacitor. The sensing electrodes 78 are pre-charged by a pre-charging circuit 79 to a predetermined voltage. When a fingertip is placed in contact with or in close proximity to the sensing electrodes 78, the capacitance is changed and this change is measured or output by addressing and output generation means 77. As in a CCD, the capacitive fingerprint imager often has circuitry for addressing each imaging sensor (sensing electrode and associated circuitry) and for converting values provided by each imaging sensor into an analogue serial signal provided as an output signal. The output signal is then sampled at a predetermined frequency in order to digitize the information and make use of it within a computer or other microprocessor based device. Alternatively, the signal can be encoded on a non-volatile storage medium such as magnetic tape for later retrieval.

When used with the present invention, it is desirable that the sensing electrodes 78 be allowed to float (unconnected to ground) when used for random value generation. The floating sensing electrodes 78 result in a signal with a substantial noise component that is

suitable for pseudo random number generation. The signal is sampled at predetermined times to produce sampled values. Random values are determined in dependence upon these sampled values. For example, the sampled values are filtered to remove ambient signals (real data) and then the remaining component (substantially noise) is evaluated. When it is above a predetermined threshold a "1" bit results. Conversely, when it is below a predetermined value a "0" bit results. It will be apparent to those of skill in the art that alternatively, a "1" bit may result from a lower value and a "0" bit from a higher value.

An embodiment of the invention will now be described in which a diffusing cover 20 is placed over an optical fingerprint sensing device in order to prevent light flicker, dust, or other variables from affecting system operation.

Referring to Fig. 3, an optical fingerprint scanner is shown comprising a biometric sensing device through which biometric input in the form of a fingerprint is received, several mirrors 12, a lens 13, and a CCD 2. The number of mirrors used is optional but is chosen so as to limit other light sources (noise) and to limit image degradation when the device is used for its intended purpose of fingerprint imaging. Optical fingerprint devices are known in the art. The biometric input device in the form of a prism acts to diffuse ambient light. Alternatively a device according to this invention is provided with a diffusing cover 20. The cover acts to diffuse light from external sources evenly across the cover.

In operation, the device is calibrated and an ambient light level is established. The calibration is performed at the beginning of each day. Alternatively, the calibration is performed at predetermined intervals throughout each day. Imaging sensors within the charge coupled device receive approximately equivalent diffused light. At least some imaging sensors are selected for use in random number generation. The imaging sensors are selected randomly. Alternatively, the imaging sensors are selected based on a statistical determination of randomness of generated values. Further alternatively, the imaging sensors are selected based on a pattern of imaging sensor selections.

It is advantageous to use a plurality of imaging sensors as described herein. Firstly, use of an array of imaging sensors provides flexibility in use, reliability from failure, and additionally, when a plurality of imaging sensors such as a CCD array is used, similar imaging sensor inputs are often easily identified to improve performance by simplifying the process of extracting random information from imaging sensor signals.

The selected imaging sensors (as well as all other imaging sensors) receive light diffused by the diffusing cover 20. The imaging sensors also receive back-scattered light in the form of noise. The noise is sufficient to effect the induced charge in at least some imaging sensors, thereby introducing noise into the CCD signal. The non-noise portion of the signal is filtered out for the selected imaging sensors and the remaining signal comprising substantially noise is evaluated. Noise values above a predetermined value are defined as "1" bits while those values below a predetermined value are defined as "0" bits. Alternatively, the noise is quantized into a 2 bit, 3 bit, ..., n bit value. Alternatively, the noise is not quantized and is used to generate analogue random values.

Referring to Figs. 4a, 4b, 4c and 4d, alternative flow diagrams for the device are shown. In Fig. 4a, the distinction between a "1" bit and a "0" bit are determined by a threshold value. As such, selected imaging sensors should have no correlation in response to ambient light or any intended stimulus having a noise component or some other substantially non-deterministic and non-repeatable component. Such a lack of correlation may occur when ambient light is constant or truly random, or where selected imaging sensors are affected by different ambient light sources. In Fig. 4a, a method is employed wherein calibration is first performed. Thereafter, a signal corresponding to intensity and frequency of light incident on imaging sensors within the CCD is provided by the CCD and a value corresponding to a predetermined imaging sensor is read. Reading a value is performed by digitizing the signal at an appropriate time. Alternatively, reading a value is performed by reading a digital value from a memory where it is previously stored. A threshold value as determined by the calibration process is compared to the read value. A value higher than the threshold value results in a '1' output and a value lower than the

threshold value results in a '0' output. Alternatively, a higher value results in a '0' output and a lower value results in a '1' output.

Advantages provided by switching imaging sensors when not random are significant. For example, when an imaging sensor is random at times or becomes stable for a while, switching to other imaging sensors provides continuous operation. Also, when a data input is provided to an imaging sensor, others potentially have no input. This is common, for example, in biometric contact imagers. Often a fingertip only covers a portion of a fingerprint scanner, for example. This allows selection of imaging sensors in corners of the imaging device wherein data input is often not provided. Of course, flexibility, reliability and ease of calibration remain significant advantages. Also, selection of a distribution for the generated sequence of random numbers is enabled according to the present method.

Referring to Fig. 4b, a flow diagram is shown for use with a CCD in the form of a video camera, optical fingerprint sensor, or other device used with a computer. During use, the device captures images of external objects and as such, there is likely a strong similarity between signals from adjacent imaging sensors within the CCD. The use of a method as exemplified by the diagram of Fig. 4a would result in "random numbers" of dubious quality. According to the method of Fig. 4b, the signal present at each imaging sensor within the CCD is measured at a high enough precision to be a measure of substantially white noise. For example, if we were to filter out all values up to 9 decimal places within the ambient signal, the resulting decimal value fluctuates in accordance with white noise and is therefore likely random.

Persons of skill in the art, would be able to test for randomness. One such series of tests is set out in Knuth, Donald E. The Art of Computer Programming, Seminumerical Algorithms Vol. 2, Addison Wesley, 1969 on pages 1-155. The analysis of the random nature of the sequences of generated values is a straightforward test requiring mere experimentation and verification. For example, a series of numbers is said to be random when a sufficiently large number of the numbers in the series exhibit

randomness. The numbers will average to the average of the desired distribution, have the desired distribution – appropriate standard deviations etc., do not follow a discernable pattern – twenty ones then twenty zeros - and so forth. Testing a device to evaluate randomness and quality of random number generation is a mere experiment and statistical analysis. Performing such an experiment and analysis allows for better selection of a filter function and a suitable threshold.

Though, for testing randomness of numbers, Knuth is suggested herein, it is solely as a reference for that purpose. Knuth provides adequate explanation of random number testing including frequency of occurrence of given numbers, average, standard deviation, variation over time, etc.; however, the specific definition of random number presented therein is not incorporated herein.

Referring to Fig. 4c, a further method of using white noise provided to or from within a plurality of imaging sensors is shown. Such a method is best applied when two imaging sensors receive substantially the same information. This is so when two microphones are placed side by side, in some adjacent imaging sensors of a CCD array, or in most imaging sensors of a CCD array when provided with light from a same source or when focused on a uniform surface. Signals from adjacent imaging sensors or other imaging sensors receiving substantially same information are read and their values subtracted to form a signal representative of substantially the white noise of one signal from one imaging sensor minus the white noise of a signal from the adjacent imaging sensor. When ambient light is present (as is the case with an optical fingerprint sensing device provided with a cover or a video camera with a diffusion covering) and no discernible non-linearities exist within the CCD field of view, each imaging sensor provides an information signal that is substantially similar to signals provided by adjacent imaging sensors. The main difference between signals from adjacent imaging sensors is attributable to noise. When such is the case, the method produces random values of good quality. Alternatively, when such is the case a value is read from each of two imaging sensors and the values are compared. The comparison results in a '0' for less than and in

a '1' for greater than. Equivalent values are either grouped into '1' or '0' or are treated as a special case, or alternatively, are included within one of the two previous cases.

There is a significant advantage to using a plurality of signals comprising noise to determine a random number, the signals from a plurality of imaging sensors. For example, the use of two signals provides a mix of two random noise values. The use of 100 signals provides a mix of 100 random noise signals. Statistically, the use of many random noise signals results in a random value even when some of those signals become somewhat deterministic or the noise therein is nominal over a period of time. As such, reliability is enhanced.

Also, the use of a number of signals from a number of different imaging sensors results in configurability not known in the prior art. Distributions become configurable by selecting and weighting different values determined based on noise portions of different signals to result in a desired distribution. This provides for a random number generator and method of generating random numbers that allows for different random number functions to be supported by a same physical device.

For example, when a distribution having a 90% chance of providing a value from 0-1 and a 10% chance of providing a value from 1-2 is desired, a first pair of signals is used to generate a random number. A second pair of signals is used to generate a second random number. Each random number has a flat distribution from 0 to 1. When the second random number is above 0.9, 1 is added to the first random number. The resulting value has the desired distribution. Of course, the signals are selected so that noise portions of the different signals are dissimilar and unrelated. Optionally, more than two signals are used for generating each random number. It is evident to those of skill in the art, that many simple and very complex random number distributions are supported by such a device.

Referring to Fig. 4d, a further method of using the white noise is shown wherein signals from each of a plurality of imaging sensors are sampled and signal values are

added to form a single value based on the output from a group of imaging sensors. The result is then compared to a threshold value to determine a random value, which is output. Alternatively, the result is further transformed prior to determining a random value. One form the further transformation can take is subtracting out higher order digits in order to limit the value to a non-ascending value; preferably, this value is comprised mostly of noise.

Referring to Fig. 4e, a further method of using white noise is shown wherein a signal from each of a plurality of imaging sensors is sampled and the sampled values are subtracted from values of sampled signals from same or similar imaging sensors from another time. For ambient light, images often remain relatively constant with the exception of slight variations and noise. Using a subtractive method of imaging sensors from a present frame from imaging sensors of a past frame (or vice versa), allows the constant nature of the frames to be exploited for extracting noise from images. The result is then compared to a threshold value to determine a random value, which is then output. Alternatively, the result is further transformed prior to determining a random value. One form the further transformation can take is subtracting out higher order digits in order to limit the value to a non-ascending value; preferably, this value is comprised mostly of noise.

Preferably, a combination of methods is concurrently available within a device or on a host computer and the selection of the method is based on a statistical analysis of randomness of the device. Alternatively, a user selects the method employed. Further alternatively, the method employed is predetermined.

It will be clear to those of skill in the art that the use of a diffusing cover is optional. In spaces where ambient light is random or relatively constant, said cover is obviated. Also, where the input device is already provided with diffusing means or means for performing a similar function, a further cover is unnecessary. It will be clear to those of skill in the art that relocating such a device requires re-calibration.

Advantageously, the device is an adaptation of an existing device. For example, another embodiment will now be described with reference to Fig. 1. When the diffusing cover 20 is replaced with a non-transmissive cover, light from the light source 6 is reflected off a platen surface of the prism 1 toward the mirror 12 and via an optical path to the imaging sensor array 2. The information content of such a signal is substantially uniform over areas of the CCD 2, and therefore over a plurality of adjacent imaging sensors. A noise portion of signals from those imaging sensors is a result of noise within the light source, noise from backscattered light, and other noise sources within the device such as inductance, capacitance, temperature, air and so forth. Using the method of Fig. 4c or Fig. 4e is particularly advantageous with such a configuration. Of course, the methods of Figs. 4a, 4b, or 4d are also applicable.

It will be clear to those of skill in the art that the use of a non-transmissive cover is optional when the prism 1 is substantially or at least partially reflective and wherein light from outside the device does not substantially affect the captured image. Alternatively, when light from outside the device does substantially affect the captured image, a method of filtering that light is used.

Referring to Fig. 5, a flow chart of a method of calibrating a system according to the present invention is shown. The system is initialized. This sets the imaging sensor array into a normal mode of operation for capturing images. A plurality of images is captured while the device is not in normal use. When a cover is used, the cover is in place prior to capturing the plurality of images. For each imaging sensor an average value is determined. Alternatively, standard deviation, average and median values are determined to ensure that the threshold value selected is statistically correct. The randomness of the values read is analyzed. This analysis includes testing for correlation among adjacent imaging sensors and distribution. Signals from any imaging sensors, which are not sufficiently random (as determined by user preference settings), are noted and associated imaging sensors are blocked out. These imaging sensors are not used by the system, at least until user preferences are changed or re-calibration occurs. The averages are stored for each imaging sensor excepting those blocked out as threshold values. Alternatively,

other values determined to be more statistically correct are stored as threshold values. Once threshold values are determined, the system is placed in a normal mode of operation.

Alternatively, when threshold values are not used, calibration is performed to verify the randomness of the noise within an imaging sensor array and to establish any correlations between imaging sensors within the array. Established correlations are then used to determine imaging sensor groupings and an applicable method of extracting noise from the signals. Further alternatively, no calibration is performed.

Where sufficient noise exists, similar methods to those set out are employable during normal use of an imaging sensor array. For example, a fingerprint sensor images a fingertip and subtracts the image from other images of the same fingertip in order to achieve a signal in dependence upon which random values are generated. Alternatively, pseudo random numbers are determined in dependence upon a specific bit or a specific digit within at least a value determined in dependence upon at least a signal from the imaging sensor array.

The random numbers generated according to the present invention are useful as seeds to pseudo-random number generators. For example, in an annealing process, it is useful to generate a random pseudo-random number. This is accomplished by generating a random seed. The seed is then provided to the user for repeating the same annealing process at a later time. Pseudo-random number generators are well known and are therefor not more fully described herein.

The invention relies on the use of an existing device connected to a computer, such as an imaging device for imaging or a touchpad for moving a cursor, for providing a signal comprising noise for use in random number generation.

Further, the invention relies on noise at each of a plurality of imaging sensors to generate a random value having a desired distribution and other desired properties. The

use of a plurality of imaging sensors in a configurable fashion as described herein is not known in the art.

In an embodiment, when a normal distribution of values is desired from a random number generator according to the invention, signals from each non-blocked imaging sensor are sampled and a distribution of noise within each signal is evaluated. Those signals that when combined result in noise having a substantially normal distribution are noted. Those same signals are then sampled during random number generation. A significant advantage of the present invention is that reconfiguring the random number generator requires little skill and no hardware modifications. To change the random number generator from a sequence having a normal distribution to one having a flat distribution requires selection of this option and possibly a re-calibration of the device.

Alternatively, several distributions are calibrated simultaneously and then a user selects a distribution as desired. As such, a calibration process may store five or six different distributions and the signals determined necessary for achieving those distributions. Upon selecting any of the distributions, the random number generation proceeds based on the determined signals.

Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.

Claims

What is claimed is:

1. A method of generating a number within a random sequence of numbers using an imaging device comprising an integrated circuit, the integrated circuit having a plurality of imaging sensors in a known arrangement for sensing an image provided thereto and for providing an output signal indicative of the sensed image, wherein the output signal comprises a plurality of pixel values each relating to an imaging sensor from the plurality of imaging sensors, each pixel value of the plurality of pixel values relating to one pixel within the sensed image at a known location dependent upon the location of the related image sensor, the method comprising the steps of:

sensing, with a first imaging sensor of the plurality of imaging sensors, a first signal to provide first sensed data, wherein at least a portion of the first sensed data comprises noise presented to or from within the device;

sensing, with a second imaging sensor of the plurality of imaging sensors, a second signal to provide second sensed data, wherein at least a portion of the second sensed data comprises noise presented to or from within the device;

determining a noise based value from the noise portion within each of the first sensed data and the second sensed data; and,

based on the noise based value providing the number within the random sequence of numbers.

2. A method of generating a number within a random sequence of numbers as defined in claim 1, comprising the step of:

comparing the noise based value to a threshold value and providing a first binary value when the noise based value is below the threshold value and a second different binary value when the noise based value is above the threshold value.

3. A method of generating a number within a random sequence of numbers as defined in claim 1, comprising the step of:

removing higher order digits from the noise based value and retaining lower order digits within the noise based value to provide the number.

4. A method of generating a number within a random sequence of numbers as defined in claim 1, wherein the step of determining a first noise based value comprises the step of: subtracting a value derived from the first sensed data from a value derived from the second sensed data to provide a difference therebetween, wherein the difference is provided as the number within the random sequence of numbers.

5. A method of generating a number within a random sequence of numbers as defined in claim 1, comprising the steps of:
extracting a combined noise portion from the first sensed data and from the second sensed data; and,
sampling the combined noise portion to produce a sampled value,
wherein the number is determined in dependence upon the sampled value.

6. A method of generating a number within a random sequence of numbers as defined in claim 1, wherein the step of determining a first noise based value comprises the steps of:
determining a primary value based on the noise portion within the first sensed data;
determining a secondary value based on the noise portion within the second sensed data; and,
based on the primary value modifying the secondary value to provide the number.

7. A method of generating a number within a random sequence of numbers as defined in claim 6, wherein modifying the secondary value comprises adding an amount to the secondary value, the amount determined in dependence upon the primary value.

8. A method of generating a number within a random sequence of numbers as defined in claim 6, wherein modifying the secondary value comprises determining a range of values for the secondary value in dependence upon the primary value.

9. A method of generating a number within a random sequence of numbers using an imaging device comprising an integrated circuit, the integrated circuit having a plurality of imaging sensors in a known arrangement for sensing an image provided thereto and for providing an output signal indicative of the sensed image, wherein the output signal comprises a plurality of pixel values each relating to an imaging sensor from the plurality of imaging sensors, each pixel value of the plurality of pixel values relating to one pixel within the sensed image at a known location dependent upon the related image sensor, the method comprising the steps of:

sensing with the plurality of imaging sensors an image provided to the device;

providing an output signal based on the sensed image; and,

In the absence of relevant image information at at least two imaging sensors of the plurality of imaging sensors:

sensing, with a first imaging sensor of the at least two imaging sensors, a first signal to provide first sensed data wherein at least a portion comprises noise presented to or from within the device;

sensing, with a second imaging sensor of the at least two imaging sensors, a second signal to provide second sensed data wherein at least a portion comprises noise presented to or from within the device;

determining a noise based value from the noise portion within each of the first sensed data and the second sensed data; and,

based on the noise based value providing the number within the random sequence of numbers.

10. A method of generating a number within a random sequence of numbers as defined in claim 9, wherein the relevant image information comprises fingerprint image data and wherein the at least two imaging sensors of the plurality of imaging sensors are placed outside an area of the image typically covered by a fingerprint.

11. A method of generating a number within a random sequence of numbers using a device comprising a plurality of sensing electrodes in a known arrangement, each sensing electrode being one of a pair of electrodes forming a capacitor, for sensing an image of an

object in contact with or in close proximity of the device, wherein the sensing electrodes sense a change of capacitance induced by the object, and for providing an output signal based on the sensed image, wherein the output signal comprises a plurality of pixel values, each pixel value of the plurality of pixel values relating to one pixel at a known location within the sensed image, the method comprising the steps of:

sensing, with a first sensing electrode of the plurality of sensing electrodes, a first signal to provide first sensed data, wherein at least a portion comprises noise presented to or from within the device;

sensing, with a second sensing electrode of the plurality of sensing electrodes, a second signal to provide second sensed data, wherein at least a portion comprises noise presented to or from within the device;

determining a noise based value from the noise portion within each of the first sensed data and the second sensed data; and,

based on the noise based value providing the number within the random sequence of numbers.

12. An imaging device used for generating a number within a random sequence of numbers comprising:

a transparent layer for transmitting impinging light in dependence upon an image provided to the imaging device;

a plurality of imaging sensors in a known arrangement within a single integrated circuit for sensing the transmitted light and for providing an output signal based on the sensed image, wherein the output signal comprises a plurality of pixel values, each pixel value of the plurality of pixel values relating to one pixel at a known location within the sensed image, and wherein at least a portion of the signal comprises white noise presented to or from within the imaging device; and,

a processor for receiving the signals from at least two imaging sensors of the imaging sensor array and for determining a value based on the portions of the signals comprising white noise.

13. An imaging device used for generating a random number as defined in claim 12, wherein the processor is for receiving the signals and for selectively determining at least two values based on a noise portion of each of the signals and wherein the random number is generated in dependence upon the two values.

14. An imaging device used for generating a random number as defined in claim 12, wherein the imaging device comprises a CCD array for sensing an image and for providing a signal including pixel values for pixels of the sensed image in each of a plurality of rows and columns.

15. An imaging device used for generating a random number as defined in claim 12, wherein the imaging device comprises a CMOS imaging device.

16. A device for generating a random number as defined in claim 14, comprising:
a prism including a platen for accepting a fingerprint;
a light source for directing light toward the platen, a portion of the light reflecting off the platen along an optical path,
wherein the charge coupled device array is disposed within the optical path to provide signals in dependence upon light within the optical path incident thereon.

17. A device for generating a random number as defined in claim 16, comprising a cover for the platen, said cover for rendering the platen substantially reflective.

18. A device used for generating a number within a random sequence of numbers comprising:
a plurality of sensing electrodes in a known arrangement, each sensing electrode being one of a pair of electrodes forming a capacitor, for sensing an image of an object in contact with or in close proximity of the device by sensing a change of capacitance induced by the object and for providing an output signal based on the sensed image,
wherein the output signal comprises a plurality of pixel values, each pixel value of the

plurality of pixel values relating to one pixel at a known location within the sensed image; and,

a processor for receiving the signals from at least two sensing electrodes of the array of sensing electrodes and for determining a value based on the portions of the signals comprising white noise.

19. A device for generating a random number as defined in claim 18, wherein the plurality of sensing electrodes is arranged in a plurality of rows and a plurality of columns each row being related to a row in the sensed image and each column being related to column in the sensed image.

20. A device for generating a random number as defined in claim 19, wherein the plurality of sensing electrodes is a touchpad.

Abstract of the Disclosure

A method and system for generating random numbers is disclosed wherein an array of imaging sensors while not in normal use, captures ambient light and back scattered light. These light sources vary naturally over a range of intensities. Intensity values above and below a threshold value are decoded as "1" and "0" bits, respectively. The resulting values, based on noise within the array signal, are single bit values or n bit values. A preferred imaging sensor array is a charge coupled device. Other imaging sensor arrays such as capacitive fingerprint imagers may also be used for this purpose when sufficient noise exists within the imaging sensor array signal.

Fig 1

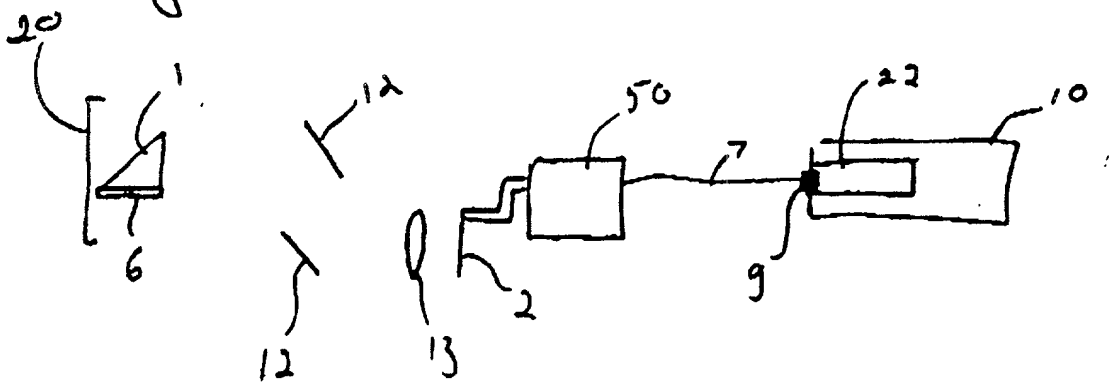
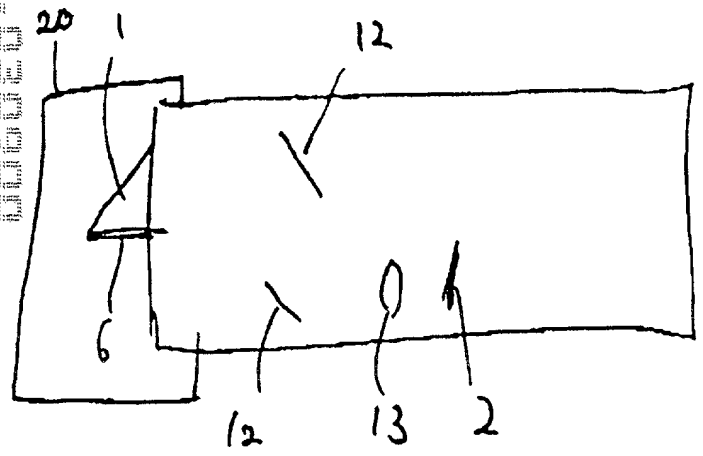
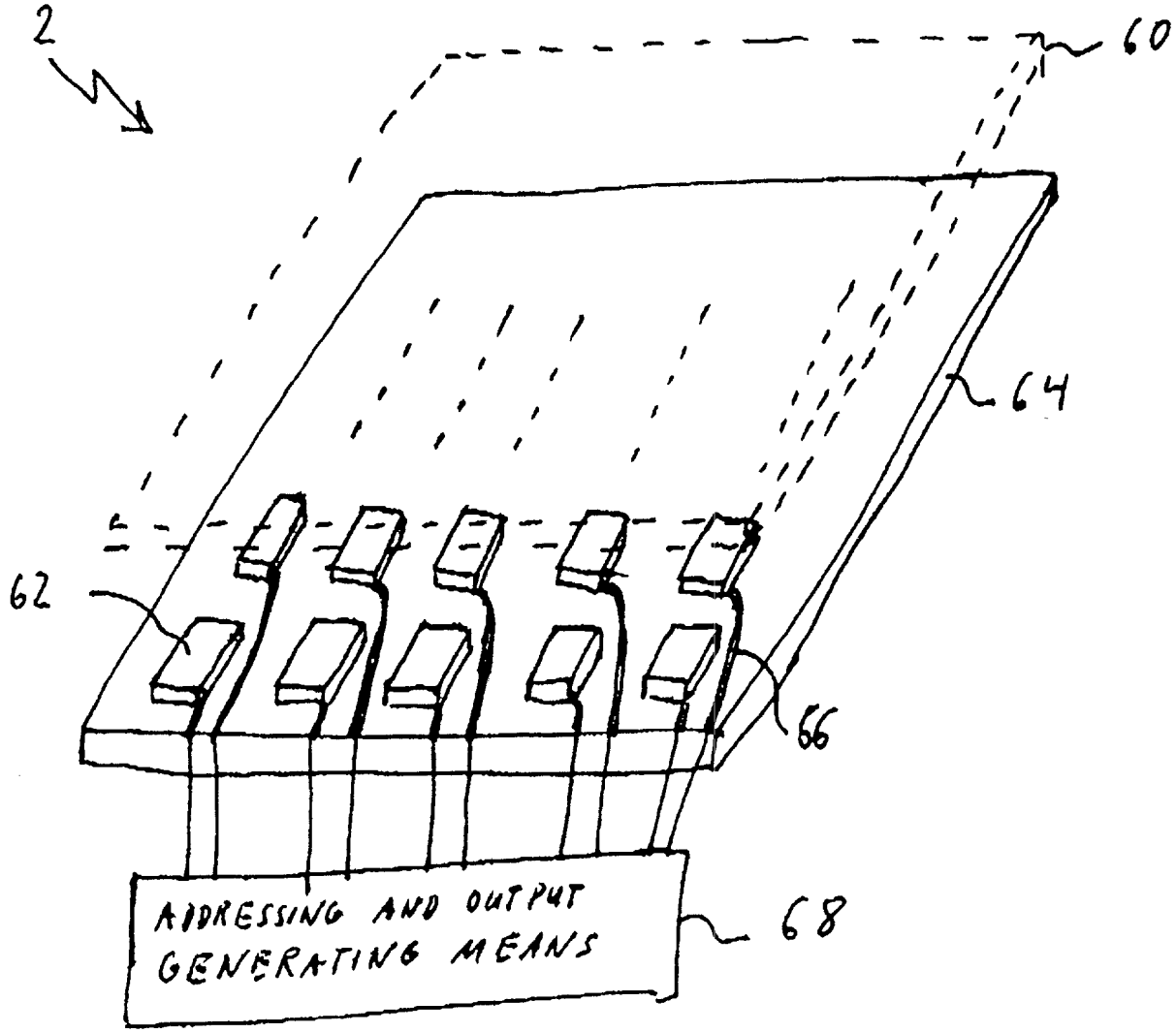


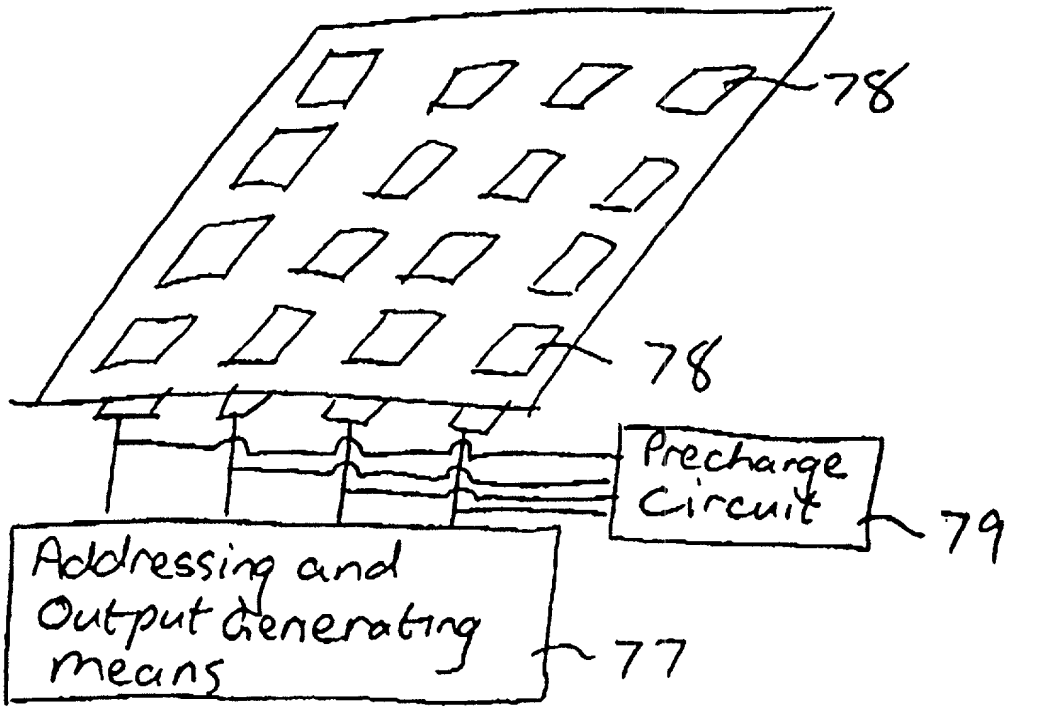
Fig 3





PRIOR ART

FIG. 1a



PRIOR ART

Fig. 2

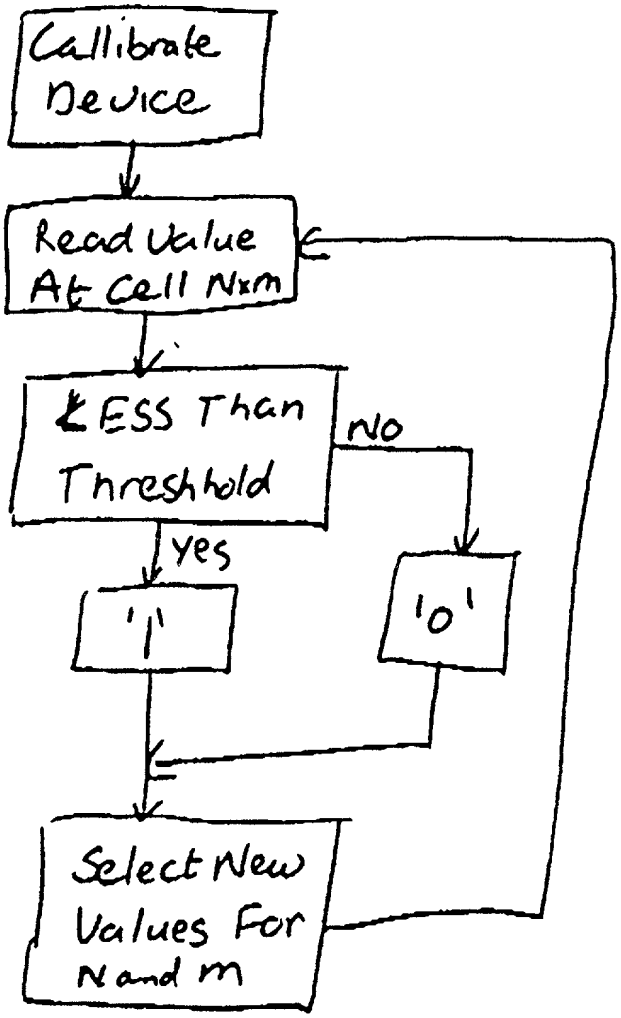

Callibrate Device
Read Value At Cell N x m
LESS Than Threshold
NO
yes
'1'
'0'
Select New Values For N and m

Fig 4A

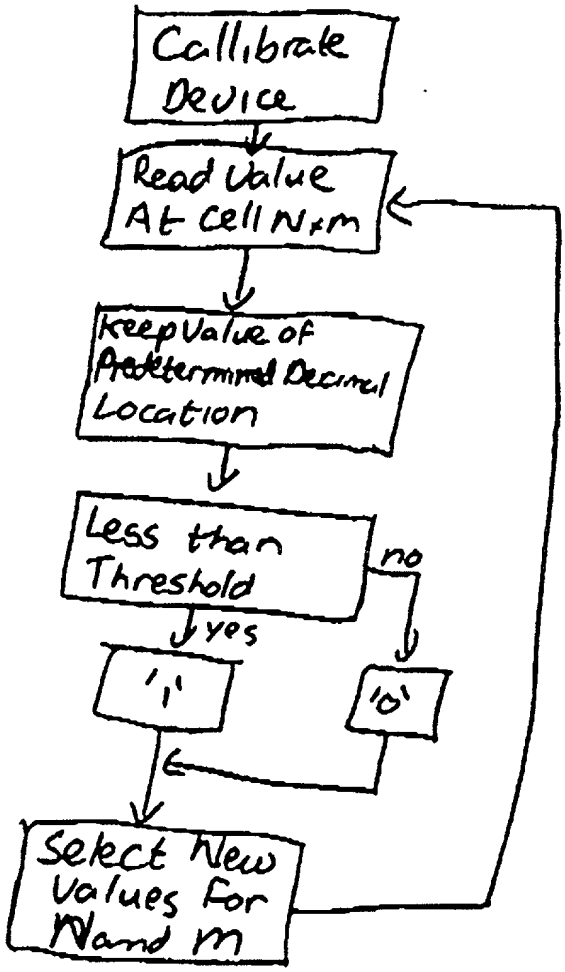

Callibrate Device
Read Value At Cell N x m
Keep Value of Predetermined Decimal Location
Less than Threshold
no
yes
'1'
'0'
Select New Values For N and m

Fig. 4B

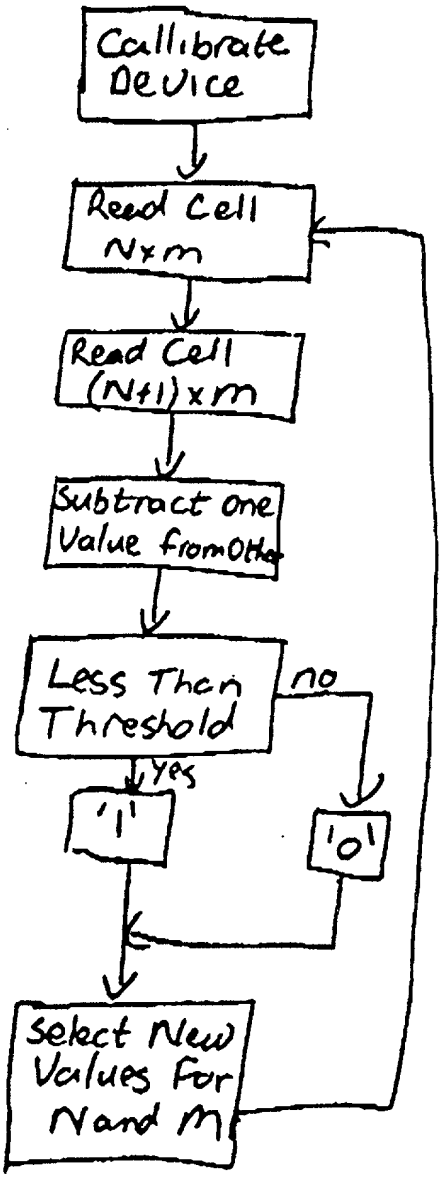

Callibrate Device
Read Cell N x m
Read Cell (N+1) x m
Subtract one Value from Other
Less Than Threshold
no
yes
'1'
'0'
Select New Values For N and M

Fig. 4C

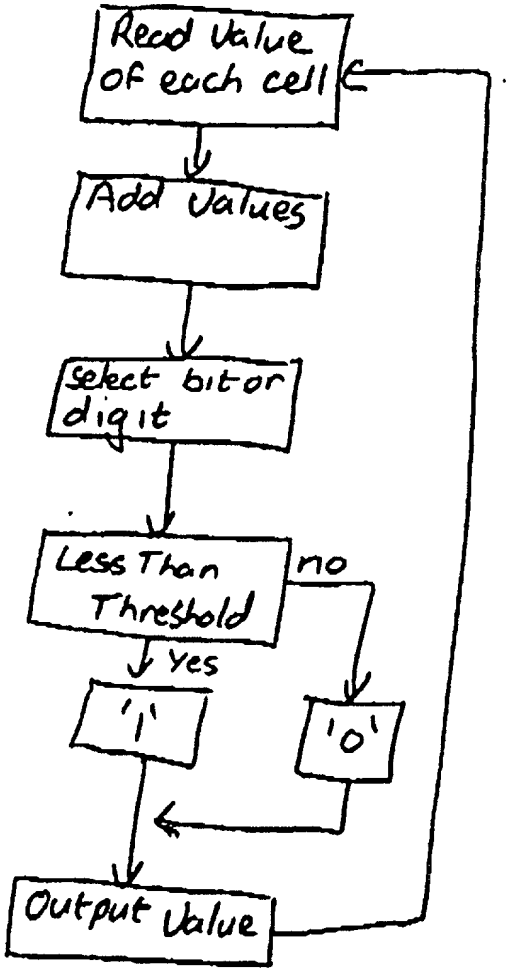

Read Value of each cell
Add Values
Select bit or digit
Less Than Threshold
no
yes
'1'
'0'
Output Value

Fig 4d

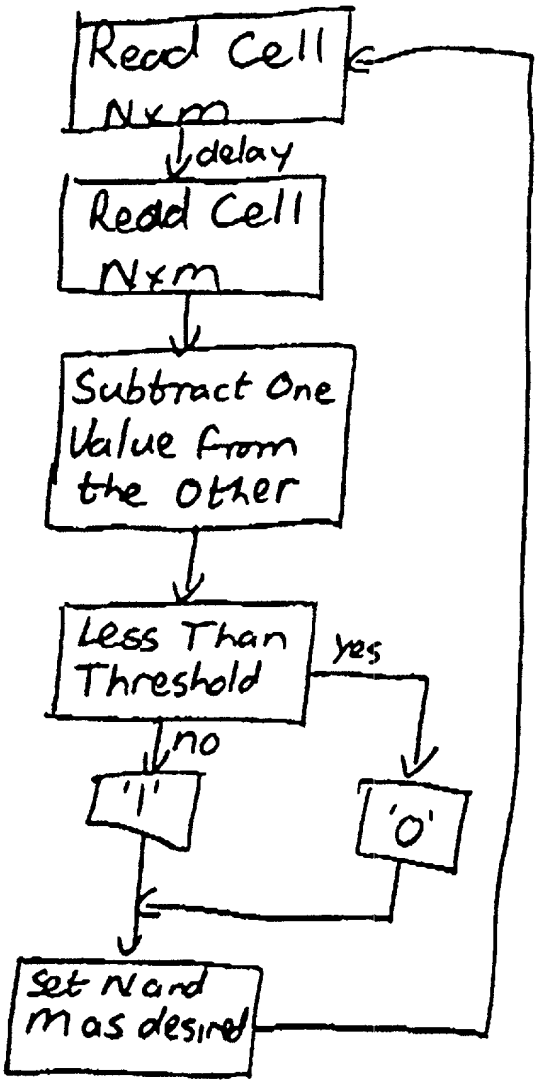
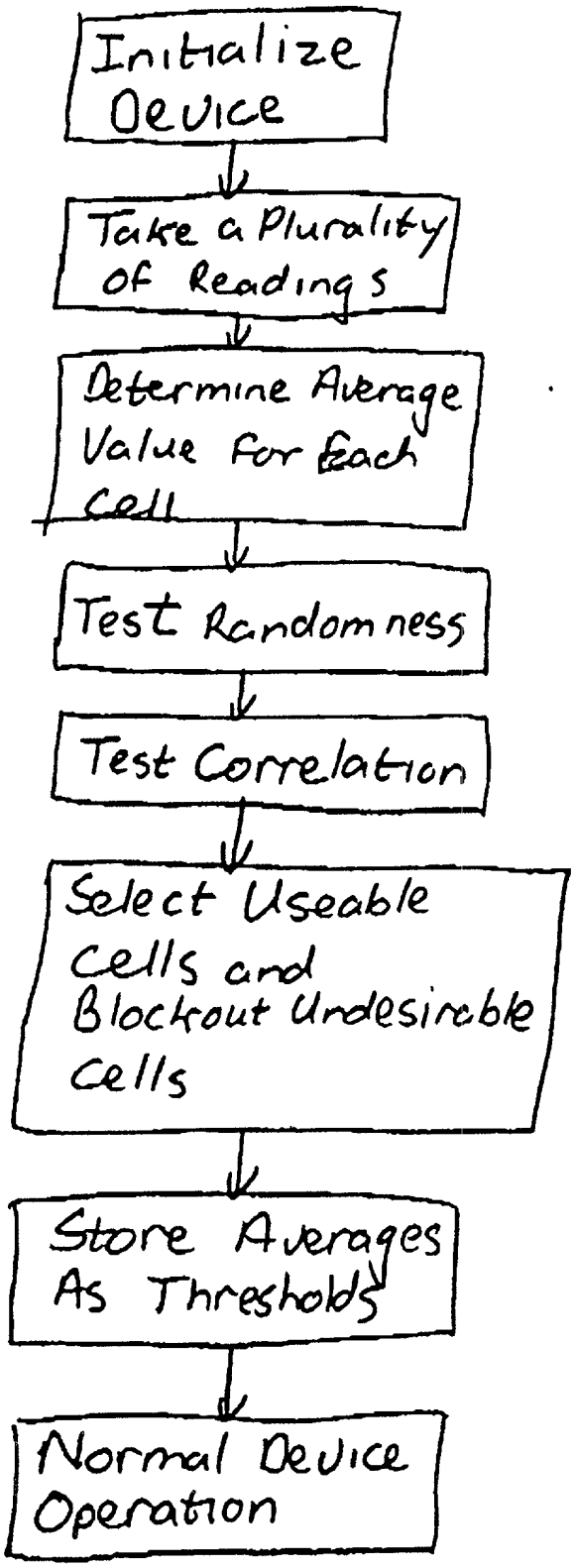

Read Cell
N x m
delay
Read Cell
N x m
Subtract One
Value from
the Other
Less Than
Threshold
yes
no
'1'
'0'
Set N and
M as desired

Fig. 4E

Fig. 5


Initialize Device
Take a Plurality of Readings
Determine Average Value for Each Cell
Test Randomness
Test Correlation
Select Useable Cells and Blockout Undesirable Cells
Store Averages As Thresholds
Normal Device Operation

File No: 12-19 US CIP(2)

DECLARATION FOR PATENT APPLICATION

As below named inventors, we hereby declare that:

Our residence, post office addresses and citizenship, are as stated below next to our names, **Stephen J. Borza** and **Gordon Freedman**.

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled

RANDOM NUMBER GENERATOR AND METHOD FOR SAME

We hereby state that we have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of the Federal Regulations, S1.56(a).

We hereby claim the benefit of Title 35, United States Code S119, of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is now disclosed in the prior United States patent application

(Number)	(Filing Date)	(Status) patented/pending/abandoned
08/728,549	**October 9, 1996**	**Abandoned**
09/023,460	**February 13, 1998**	**Pending**

We hereby appoint the following agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Gordon Freedman **Regn. No: 41,553**
Neil Teitelbaum **Regn. No. 38,793**
At telephone number: **(613) 228-2838**

Address all correspondence to: **Gordon Freedman**
Freedman & Associates
54 Cimarron Crescent
Nepean, Ontario
Canada
K2G 6C9

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: **Stephen J. Borza**

Inventor's signature: Stephen J Borza. Date: 17 Dec 99

Residence: **495 Metcalfe Street, Ottawa, Ontario, Canada, K1S 3N3**
Post Office Address: **Same as above**

Citizenship: **Canadian**

Full name of second inventor: **Gordon Freedman**

Inventor's signature: Date:

Residence: **54 Cimarron Crescent, Nepean, Ontario, Canada K2G 6C9**
Post Office Address: **Same as above**

Citizenship: **Canadian**

Gordon Freedman	**Regn. No: 41,553**
Neil Teitelbaum	**Regn. No. 38,793**
At telephone number:	**(613) 228-2838**

Address all correspondence to: **Gordon Freedman**
Freedman & Associates
54 Cimarron Crescent
Nepean, Ontario
Canada
K2G 6C9

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of first inventor: **Stephen J. Borza**

Inventor's signature: Date:

Residence: **495 Metcalfe Street, Ottawa, Ontario, Canada, K1S 3N3**
Post Office Address: **Same as above**

Citizenship: **Canadian**

Full name of second inventor: **Gordon Freedman**

Inventor's signature: Date: Dec. 15/99

Residence: **54 Cimarron Crescent, Nepean, Ontario, Canada K2G 6C9**
Post Office Address: **Same as above**

Citizenship: **Canadian**